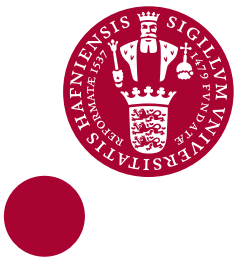

Liability (and) Rules for Health Information

Contreras, Jorge; Nordfalk, Francisca

Published in:
Health matrix (Cleveland, Ohio : 1991)

Publication date:
2019

Document version
Publisher's PDF, also known as Version of record

Masthead Logo

Health Matrix: The Journal of Law-Medicine

Volume 29 | Issue 1

2019

Liability (and) Rules for Health Information

Jorge L. Contreras

Francisca Nordfalk

Liability (and) Rules for Health Information

Jorge L. Contreras[†] *& Francisca Nordfalk*[††]

Abstract

The recent trend toward propertization of health data could pose significant challenges to biomedical research and public health. Property rule systems can result in sizable up-front costs in the acquisition of consent from individual data subjects, as well as the ongoing risk that data subjects will retract consent or object to unanticipated data uses, thus compromising existing data resources and analyses. Instead, we propose that research using individual health data should be subject to a regulatory regime, enforceable by government/public repositories, while at the same time permitting private enforcement actions to address particularized individual injury. Thus, while the physical collection of human tissue would continue to be subject to existing rules regarding informed consent, ex ante consent would not be required for the use of information derived from physical samples. Rather, rules regarding permissible research use and handling of health information would be put in place, and violations of those rules would be dealt with on an ex post basis, both through regulatory penalties and private liability actions. These recommendations are supported by two cases studies: the Utah Population Database and Statistics Denmark, both of which provide examples of successful health data repositories that are governed by regulatory systems. While these examples are drawn from governmental data resources, the approach that they exemplify can be extended to academic and other research environments. These case studies suggest that regulatory and liability

† JD (Harvard Law School), BSEE, BA (Rice University), Professor, University of Utah S.J. Quinney College of Law; Adjunct Professor, University of Utah School of Medicine, Department of Human Genetics.

†† PhD Candidate, Section for Health Services Research, Department of Public Health, University of Copenhagen. Valuable comments and discussion of this Article were provided by Gideon Parchomovsky, Jesse Reynolds, Nadya Purtova, Jed Shugerman and Tori Smith. This Article benefitted from presentation and feedback at the Association of Law, Property, and Society 9th Annual Meeting at Maastricht University and faculty workshops at Fordham Law School, Tilburg University and Nottingham-Trent University. Research assistance by Ross McPhail and Rick Rose is greatly appreciated. Contreras received partial support for this research from the Huntsman Cancer Institute/Huntsman Cancer Foundation and the Utah Center for Genomic Innovation. This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement number 682110).

models should be considered more broadly for the governance of research using human health data in lieu of property-based systems.

CONTENTS

INTRODUCTION

In the wake of recent scandals involving the use and abuse of individual data by commercial entities,[1] a number of new proposals

1. *See generally* Taylor Amerding, *The 17 Biggest Data Breaches of the 21st Century*, CSO (Jan. 26, 2018), https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html; Alexis C. Madrigal, *What We Know About Facebook's Latest Data Scandal*, THE ATLANTIC (Jun. 4, 2018), https://www.theatlantic.com/technology/archive/2018/06/what-we-know-about-facebooks-latest-data-scandal/561992/; Jennifer Dudley-Nicholson, *Social Media Data Scandal: It's Not Just Facebook*, FRASER COAST CHRON. (May 1, 2018),

have emerged to recognize personal property interests in individual health data. These proposals have largely been made by aspiring data intermediaries that would employ technologies such as Blockchain[2] to enable consumers to control the flow of their personal health data. The intermediaries would then act as the consumers' representative in selling that data to healthcare providers, pharmaceutical manufacturers, and anyone else interested in it, remitting a portion of the revenue back to the consumer.[3] The linchpin of this attractive new business model is establishing individual ownership of personal data. Without ownership, companies, hospitals, insurers, and data intermediaries can (and today do) aggregate and sell individual health information without consulting, or paying, the individual.[4] But if consumers *owned* their data, then anyone that tried to use or sell it without permission would be stealing (or at least liable for the tort of conversion).

The notion of individual data ownership seems to be catching on. A handful of U.S. states have enacted legislation purporting to give individuals ownership over their genetic information.[5] Even former

https://www.frasercoastchronicle.com.au/news/social-media-data-scandal-its-not-just-facebook-bu/3403026/.

2. Blockchain in a relatively new, "tamperproof" form of technology, famously employed by bitcoin. Arjun Kharpal, *Everything You Need to Know About the Blockchain*, CNBC (Jun. 18, 2018), https://www.cnbc.com/2018/06/18/blockchain-what-is-it-and-how-does-it-work.html. *See also* Megan Molteni, *These DNA Startups Want to Put All of You on the Blockchain*, WIRED (Nov. 16, 2018), https://www.wired.com/story/these-dna-startups-want-to-put-all-of-you-on-the-blockchain/.

3. *See, e.g.*, Megan Scudellari, *Get Paid for Your Genetic Data*, IEEE SPECTRUM (Mar. 1, 2018), https://spectrum.ieee.org/the-human-os/biomedical/diagnostics/paying-for-genetic-data-with-cryptocurrency (describing plans by start-up Nebula Genomics to enable consumers to own and sell access to their data to pharmaceutical companies using Blockchain technology); Ron Miller, *Hu-manity Wants to Create a Health Data Marketplace With Help From Blockchain*, TECHCRUNCH (Jul. 18, 2018), https://techcrunch.com/2018/07/18/hu-manity-wants-to-create-a-health-data-marketplace-with-help-from-blockchain/; Misha Angrist, *Do You Belong to You*? GENOME, Jan. 2, 2018, at 44-45 (discussing Genos, which claimed that customers would retain ownership of their exome data while receiving "transparent compensation for research studies in which they participate[d]"); Leonard J. Kish & Eric J. Topol, *Unpatients – Why Patients Should Own Their Medical Data*, 33 NATURE BIOTECHNOLOGY 921, 923 (2015) [hereinafter Kish & Topol, *Unpatients*] ("we have proposed a technological solution that allows biomedical data to be shared and traded as property at a very granular level").

4. Miller, *supra* note 3; s*ee* Kish & Topol, *Unpatients, supra* note 3, at 922.

5. *See* Anya E.R. Prince, *Comprehensive Protection of Genetic Information: One Size Privacy or Property Models May Not Fit All*, 79 BROOKLYN L. REV. 175, 195–98 (2013) (discussing statutory enactments in Alaska, Colorado, Georgia, Louisiana, and Florida). *But see* OR. PUBLIC HEALTH

President Barack Obama expressed the view that "if somebody does a test on me or my genes . . . that's mine."[6]

But despite its rhetorical and populist appeal, the recent trend toward propertization of personal health information could pose significant challenges to both biomedical research and public health. Assigning property rights to personal information could result in researchers incurring (or being unable to afford) sizable up-front costs to acquire permission to conduct most forms of data-based research and could limit the amount of data that public health officials can collect and utilize for the public benefit. Moreover, the hallmark of personal property -- the right to exclude -- poses an ongoing risk that individuals could retract or narrow their consent to data use after it has been given, thus compromising existing data resources and analyses.

In their landmark *Harvard Law Review* article,[7] Guido Calabresi and Doug Melamed elucidate the now-familiar dichotomy between property rules and liability rules. Property rules, they explain, permit the holder of an entitlement (a property interest) to prevent others from encroaching on the enjoyment of that entitlement, just as a landowner may prevent trespassers from entering his land.[8] Liability rules, on the other hand, do not grant an *a priori* entitlement to prevent trespass, but do provide the aggrieved party with a legal remedy (usually damages) if such an encroachment occurs (i.e., allowing the land owner to recover monetary damages as compensation for a trespass).[9] Since its introduction to the literature, this distinction has shed light on the nature of legal rules and rulemaking in contexts ranging from air pollution,[10] to accidents,[11] to intellectual property,[12] to database

---

DIV., HISTORY OF OREGON'S GENETIC PRIVACY LAW 1-3 (2007) (discussing 1995 enactment and 2001 repeal of genetic property legislation in Oregon).

6. Julie Hirschfeld Davis, *President Weighs in on Data from Genes*, N.Y. TIMES, Feb. 25, 2016, at A15. *But see* Jorge L. Contreras, *Letter to the Editor: The President Says Patients Should Own Their Genetic Data. He's Wrong.* 34 NATURE BIOTECHNOLOGY 585, 585-586 (2016) [hereinafter Contreras, *Letter*] (criticizing this view).

7. Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1089 (1972).

8. *Id.* at 1092.

9. *Id.* at 1105–06, 1116, 1119–20.

10. *See id.* at 1115-24.

11. *See, e.g.*, GUIDO CALABRESI, THE COST OF ACCIDENTS 3 (1970); STEVEN SHAVELL, ECONOMIC ANALYSIS OF ACCIDENT LAW 130 (1987).

12. *See, e.g.*, Dan L. Burk & Mark A. Lemley, *Policy Levers in Patent Law*, 89 VA. L. REV. 1575, 1665 (2003); Dan Burk, *Muddy Rules for Cyberspace*, 21 CARDOZO L. REV. 121, 124-28 (1999).

protection,[13] to criminal law.[14] In prior work, Contreras extended this analysis to human genetic data,[15] and Jane Baron has touched on its implications for electronic health records.[16]

In this article, we argue that property rule frameworks are inadequate and inappropriate for the governance of human health data.[17] Instead, we support a combination of regulatory governance coupled, in some circumstances, with private liability remedies. In support of this structure, we introduce two new case studies from health data repositories in the United States (the Utah Population Database) and Denmark (Statistics Denmark) in which regulatory approaches have been utilized successfully to safeguard individual privacy and data security while at the same time promoting the research enterprise. We thus recommend that these models be considered more broadly for the governance of human health data.

The remainder of this article proceeds in three principal parts. Part I summarizes recent trends toward propertization of health data, both in the literature and in U.S. litigation. Part II summarizes the theoretical frameworks for allocating initial entitlements and controlling risk introduced by Calabresi and Melamed and by Steven Shavell, and then explores an alternative framework for health data, including an analysis of available remedies and the role of public authorities in monitoring and enforcing such rules. Part III presents two case studies in which regulatory frameworks have successfully been used for health data: the Utah Population Database and Statistics Denmark. We conclude with recommendations and directions for future research.

---

13. J. H. Reichman & Paul F. Uhlir, *A Contractually Reconstructed Research Commons for Scientific Data in a Highly Protectionist Intellectual Property Environment*, 66 L. & CONTEMP. PROBS. 315, 387 n.372, 395, 410 (2003).

14. *See* Calabresi & Melamed, *supra* note 7, at 1124-27; Richard A. Posner, *An Economic Theory of the Criminal Law*, 85 COLUM L. REV. 1193 (1985).

15. Jorge L. Contreras, *Genetic Property*, 105 GEO. L.J. 1 (2016).

16. Jane B. Baron, *Property as Control: The Case of Information*, 18 MICH. TELECOMM. & TECH. L. REV. 367, 380 (2012).

17. Individual health information includes a wide range of elements including medical records, test results, clinical data, tissue samples, and data concerning an individual's age, health history, family history, community, ethnicity, and other demographic information. For an excellent discussion of these data types, see Barbara J. Evans, *Much Ado About Data Ownership*, 25 HARV. J. L. & TECH. 69, 90–2 (2011). The extension of data sharing and similar principles from the field of genomics to health information more generally is discussed in Jorge L. Contreras & Bartha M. Knoppers, *The Genomic Commons*, 19 ANN. REV. GENOMICS & HUMAN GENETICS 429, 431-32 (2018).

I. PROPERTY RULES AND HEALTH DATA

A. The Propertization of Health Data

Traditionally, U.S. law has treated the use of information, once it is disclosed,[18] as free from property entitlements. No property interest exists in facts or information once they are generally known.[19] Rather, facts are part of the public domain, described by Justice Louis Brandeis as "free as the air to common use."[20] The unencumbered status of information has been recognized in cases involving not only current news[21] and sports scores,[22] but also genetic and other health data. In *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, the Supreme Court held that the information contained in naturally occurring human DNA molecules cannot be patented.[23] Likewise, in cases including *Moore v. Regents of the University of California*,[24] *Washington University v. Catalona*,[25] and *Greenberg v. Miami Children's Hospital Research Institute, Inc.*,[26] federal and state courts

18. The law of trade secrets addresses information that is both commercially valuable and held in confidence. Trade secrets, which are commonly viewed as "intellectual property," derive their value, if not their very existence, from their secrecy. *See* Susan C. Miller, *Florida's Uniform Trade Secret Act*, 16 FLA. ST. L. REV. 863 (1988). The focus of this paper, however, is on information that is disclosed or derived in a manner that is beyond the scope of trade secret protection. In particular, the following categories of information about an individual would not normally be considered trade secrets: information that the individual has previously disclosed or which is a matter of public record (e.g., address, birth date), information that is observable either to the naked eye or upon a medical examination, information that is derived from the analysis of an individual's tissue or DNA. These categories of information, to the extent that they are legally protected are protected under laws and regulations pertaining to privacy, as discussed below.

19. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 344–45 (1991); Int'l News Serv. v. Associated Press, 248 U.S. 215, 234 (1918).

20. Int'l News Serv., 248 U.S. at 250 (Brandeis, J., dissenting).

21. *Id.* at 234.

22. *See* Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 853 (2d Cir. 1997).

23. Ass'n for Molecular Pathology v. Myriad Genetics, Inc., No. 12–398, slip op. at 10-18 (U.S. June 13, 2013).

24. Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 493 (Cal. 1990).

25. Washington Univ. v. Catalona, 490 F.3d 667, 673 (8th Cir. 2007).

26. Greenberg v. Miami Child. Hosp. Res. Inst., 264 F. Supp. 2d 1064, 1074 (S.D. Fla. 2003) (Plaintiffs provided Defendants with tissue and health information that Plaintiffs intended for Defendants to use to research a specific disease. Without the Plaintiff's knowledge, Defendants submitted a patent application for a genetic sequence identified. The court did not recognize that Plaintiffs had any legal claim to the fruits of the research).

have refused to recognize a personal property interest in discoveries and information obtained through the analysis of human biological material, irrespective of whether or not that material was obtained legally.[27]

The trend toward data propertization has also been seen in Europe. Despite a general legal understanding in most European countries that data is not itself subject to property protection,[28] the new European General Data Protection Regulation imposes significant protections for individual data including the right for individuals to exert rights of portability and erasure over data about themselves.[29] As recently observed by Nadya Purtova, these features offer a regulatory framework that bears a strong resemblance to a property rule system.[30]

Notwithstanding the general principle that unprotected data is not a form of property, there has recently been a resurgence of interest in treating individual health information under a property rule framework.[31] Numerous scholars, policymakers, and advocates, drawing on earlier debates concerning property interests in personal information, generally,[32] as well as the ownership of human tissue, body parts and

27. In *Moore*, for example, the court found that Mr. Moore's physician at UCLA committed both deception and violation of his fiduciary duty. Nevertheless, the court declined to recognize a property interest in Mr. Moore's extracted cells and tissue or the discoveries made with them. *See* Moore v. Regents of the Univ. of California, 793 P.2d 479, 493 (Cal. 1990).

28. *See* John Rumbold & Barbara Pierscionek, *Why Patients Shouldn't "Own" Their Medical Records*, 34 NATURE BIOTECH. 586, 586 (2016).

29. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/E*C [hereinafter GDPR].*

30. *See* Nadezhda Purtova, *Do Property Rights in Personal Data Make Sense After the Big Data Turn?* 10 J. L. ECON. REG. 208, 214 (2017).

31. *See, e.g.*, Angrist, *supra* note 3, at 43; Mark A. Rothstein, *Ethical Issues in Big Data Health Research*, 43 J.L. MED. & ETHICS 425, 427 (2015) ("many individuals strongly believe that their biological specimens and health records 'belong to them.'"); Richard H. Thaler*, Show Us the Data. (It's Ours, After All),* N.Y. TIMES (Apr. 23, 2011), https://www.nytimes.com/2011/04/24/business/24view.html; Evans, *supra* note 17, at 73 (citing media calls for patient ownership of health data).

32. *See, e.g.*, Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2094 (2004) (proposing a five-part framework defining rights in personal information); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 228 (2006) (proposing a property-based framework to protect online privacy); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1379 (2000) [hereinafter Cohen, *Examined Lives*]; Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1289 (2000).

indigenous resources,[33] have argued that property rights in genetic data and other health information should be legally recognized. The rationales marshalled in favor of data propertization are varied, ranging from concerns over individual autonomy; privacy and dignity;[34] to enabling individuals to sell their data and thus share in the financial rewards reaped by others (e.g., pharmaceutical firms);[35] to offering an alternative (and an antidote) to the increasing control of personal data by large corporations;[36] to considerations of group dynamics and social interactions;[37] to enabling patients to access information about

33. *See, e.g.,* R. Alta Charo, *Body of Research – Ownership and Use of Human Tissue*, 355 N. ENG. J. MED. 1517 (2006).

34. *See, e.g.*, Jessica L. Roberts, *Progressive Genetic Ownership*, 93 NOTRE DAME L. REV. 1105, 1158-59 (2018) (summarizing arguments *re* autonomy, privacy, identity); Leonard J. Kish & Eric J. Topol, *Correspondence*, 34 NATURE BIOTECH. 586, 587 (2016) [hereinafter Kish & Topol, *Correspondence]* (responding to Rumbold & Pierscionek, *supra* note 28) ("Our personal autonomy increasingly depends upon our digital autonomy").

35. *See, e.g.,* Roberts, *supra* note 34, at 1164 ("legally recognized genetic ownership rights could result in financial compensation . . . Sources of genetic data would enjoy some measure of wealth in the exchange"); Kish & Topol, *Unpatients*, *supra* note 3, at 923 ("To build a truly thriving health data economy, we need to harness the power of data ownership"); Mark A. Hall & Kevin A. Schulman, *Ownership of Medical Information*, 301 J. AM. MED. ASS'N 1282, 1284 (2009) (the assignment of "economic value to the access, control, and use of the medical information contained in electronic health record networks" would empower patients); David F. Partlett, *Misuse of Genetic Information: The Common Law and Professionals' Liability*, 42 WASHBURN L.J. 489, 497 (2003) ("If the genetic information is property, it can presumably be sold, leading to a market in the information."); Bartha Maria Knoppers, *Population Genetics and Benefit Sharing*, 3 COMMUNITY GENETICS 212, 213 (2000) (collecting statements on benefit sharing from international organizations including WHO, UNESCO, HUGO); Anita L. Allen, *Genetic Privacy: Emerging Concepts and Values, in* GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA 31, 51 (Mark A. Rothstein ed., 1997) (allowing individuals to sell their genetic information could enable them to participate in the market and avoid exploitation by others).

36. *See, e.g.*, Purtova, *supra* note 30, at 218 ("digital giants like Google and Facebook harvest, hoard, hold monopoly over and exclusively profit from the pools of data collected through their various services, whereas these pools are not available to anyone else . . . . Allocating property rights in personal data to individuals . . . will arguably help avoid this enclosure").

37. *See, e.g.*, Natalie Ram, *DNA by the Entirety*, 115 COLUM. L. REV. 873, 906–10 (2015) (proposing that DNA be owned through a "tenancy by the entirety" joint ownership model in order to account for the interests of related family members); Laura Maria Franciosi & Attilio Guarneri, *The Protection of Genetic Identity*, 1 J. CIV. L. STUD. 139, 186 (2008) ("[P]roperty laws may better serve as a paradigm to ensure that a greater

themselves that is not currently available from their healthcare providers.[38]

These policy positions have also been advanced by litigants seeking to assert property interests in human genetic information and related biological samples. Notably, in *Beleno v. Lakey*, four Texas families sued the State of Texas for unauthorized use of blood samples routinely collected from newborns as part of a state program to screen for birth defects.[39] The families brought suit when they discovered that, following the initial screening, the state continued to store and use these samples for purposes of epidemiological, environmental exposure and other research.[40] They claimed, among other things, that the state's failure to obtain their express consent to ongoing research violated their privacy and other rights.[41] In settling the litigation, the state agreed to destroy its entire repository of 5.3 million infant blood samples, eliminating any possibility of their use in future research.[42] Similar lawsuits have been brought in other states[43] and have led, among other things, to the enactment of the federal Newborn Screening Saves Lives

level of protection is provided for information that belongs to all of the individuals involved.").

38. Kish & Topol, *Unpatients, supra* note 3, at 922 ("the US legal framework is constructed in a manner to block individuals from accessing their own medical data"); Kish & Topol, *Correspondence*, *supra* note 34, at 587 (discussing example of a patient who was unable to obtain data from the manufacturer of his own implanted defibrillator).

39. *See* Beleno v. Lakey, 306 F.Supp.3d 930, 936 (W.D. Tex. 2009). For a history of newborn blood screening programs, see Sonia M. Suter, *Did You Give the Government Your Baby's DNA? Rethinking Consent in Newborn Screening*, 15 MINN J.L. SCI. & TECH. 729, 734–37 (2014).

40. Peggy Fikac, *State to Destroy Newborns' Blood Samples*, HOUS. CHRON. (Dec. 22, 2009), http://www.chron.com/news/houston-texas/article/State-to-destroy-newborns-blood-samples-1599212.php; *see generally* Suter, *supra* note 39, at 754–57 (describing additional research uses of newborn blood spots).

41. Beleno, 306 F.Supp.3d at 936. In Texas, participation in the screening program was required by law, with a right to opt-out for religious reasons only. *See* Suter, *supra* note 39, at 784.

42. Adam Doerr, *Newborn Blood Spot Litigation: 70 Days to Destroy 5+ Million Samples*, PRIVACY REP. (Feb. 2, 2010), https://theprivacyreport.com/2010/02/02/newborn-blood-spot-litigation-70-days-to-destroy-5-million-samples/; Fikac, *supra* note 40.

43. *See, e.g.*, Bearder v. State, 806 N.W.2d 766, 776 (Minn. 2011) (deciding the use of newborn blood spots for research purposes without consent violated Minnesota law). *See generally* Suter, *supra* note 39, at 757–59 (discussing state cases challenging infant blood spot collection and storage).

Reauthorization Act of 2014, which requires explicit parental consent for all research on newborn blood samples.[44]

Another recent case involved the Havasupai Indian Tribe. In 1989, representatives of the tribe approached researchers at Arizona State University (ASU) to investigate high rates of diabetes among tribe members.[45] The researchers collected approximately 200 blood samples from members of the tribe using an informed consent document that purported to authorize research concerning "the causes of behavioral/medical disorders."[46] By 1991, the researchers concluded that there was no genetic link to the high incidence of diabetes within the tribe.[47] After the initial study, other ASU researchers continued to use the DNA collected from tribe members in other research projects, including investigations of schizophrenia and ancient human migratory patterns.[48] When the tribe learned of this additional research it sued ASU for $50 million, claiming that the non-diabetes research was unauthorized and constituted a breach of fiduciary duty, fraud, negligence, and trespass to chattels.[49] The parties settled the suit in 2010, with ASU paying $700,000 to forty-one tribe members and agreeing to return all remaining DNA to the tribe.[50] Several other documented cases exist in which research has been curtailed or discontinued after complaints were lodged by representatives of tribal or other local groups that contributed original biological specimens for research.[51]

These cases demonstrate that research participants have increasingly asserted[52] broad rights to prevent "their" data from being

44. Newborn Screening Saves Lives Reauthorization Act of 2014, Pub. L. No. 113-240, 128 Stat. 2851 (2014); 45 C.F.R. § 46.408 (2019).

45. Havasupai Tribe v. Ariz. Bd. of Regents, 204 P.3d 1063, 1066 (Ariz. Ct. App. 2008). A summary of the background and facts of the case can be found in Leslie E. Wolf, *Biology & Genetics: Advancing Research on Stored Biological Materials: Reconciling Law, Ethics, and Practice*, 11 MINN J.L. SCI. & TECH. 99, 118–125 (2010).

46. Michelle M. Mello & Leslie E. Wolf, *The Havasupai Indian Tribe Case—Lessons for Research Involving Stored Biologic Samples*, 363 NEW ENGL. J. MED. 204, 204 (2010).

47. Havasupai, 204 P.3d at 1067.

48. *Id.*

49. *Id.* at 1069–71.

50. *See* Jennifer Couzin-Frankel, *DNA Returned to Tribe, Raising Questions About Consent*, 328 SCIENCE 558, 558 (2010); Mello & Wolf, *supra* note 46, at 204-05.

51. *See, e.g.*, Couzin-Frankel, *supra* note 50.

52. Both the *Beleno* and *Havasupai* cases were settled by the parties prior to the courts' rulings on the merits. Beleno v. Lakey, 306 F.Supp.3d 930, 936 (W.D. Tex. 2009); Havasupai Tribe v. Ariz. Bd. of Regents, 204 P.3d 1063, 1066 (Ariz. Ct. App. 2008).

used for unauthorized purposes, even when the use of that data poses no meaningful physical or psychological threat to them.[53] They also suggest that earlier precedents such as *Moore*[54] and *Greenberg*,[55] which rejected property-like ownership of individual data, are at risk of being eroded in the current legal climate.

B. Informed Consent and Property Rules for Data Research

The principal mechanism through which property-like control over human health data has emerged is an increasingly expansionist view of the doctrine of informed consent. This doctrine, which took its current form in response to abuses committed by researchers both during and after World War II, offers necessary protections to the human subjects of medical experimentation.[56] But this otherwise essential doctrine has been expanded beyond its original contours to become what Contreras has referred to as "propertizing consent."[57] With propertizing consent, the permission sought from an individual to undergo a medical procedure, including something as simple as a cheek swab or blood draw, invests that individual with a property-like interest in all resulting data. A requirement that advance permission for the use of data be sought before research can commence is akin to giving an individual an ownership interest in all information about himself or herself. The reliance on individual consent for data-based research, which is unlikely to cause physical or psychological harm to the individual, enables the individual to exert a property-like right to exclude with respect to that data.

The informed consent requirement and other human research protections are currently codified under U.S. law as part of the so-called "Common Rule" that applies to all federally funded research concerning human subjects.[58] Alongside the Common Rule is the HIPAA Privacy Rule, which establishes detailed regulations regarding the collection, use, storage, and disclosure of protected health information (PHI) by healthcare providers, laboratories, payers, and other "covered entities."[59] While numerous exceptions and exemptions under the

53. For a discussion of the potential threats alleged to accompany data-based research, see Contreras, *Genetic Property, supra* note 15, at 44-48.

54. Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 488-93 (Cal. 1990).

55. Greenberg v. Miami Child. Hosp. Res. Inst., 264 F. Supp. 2d 1064, 1074 (S.D. Fla. 2003).

56. *See* NAT'L COMM'N FOR THE PROTECTION OF HUMAN SUBJECTS OF BIOMEDICAL & BEHAV. RES., THE BELMOND REPORT: ETHICAL PRINCIPLES AND GUIDELINES FOR THE PROTECTION OF HUMAN SUBJECTS OF RESEARCH (1979).

57. Contreras, *Genetic Property, supra* note 15, at 6-7.

58. General Requirements for Informed Consent, 45 C.F.R. § 46.116 (2019).

59. 45 C.F.R. §§ 160, 164 (2019).

Common Rule and HIPAA Privacy Rule may be applied to research using human health data that has been de-identified (stripped of identifying data that can be linked back to individuals), these exceptions are complex, incomplete, and subject to differing interpretations.[60] Moreover, there is increasing criticism of the informed consent requirement itself, given that current consent documentation, like computer click-through agreements, are lengthy and legalistic, neither giving the average consumer useful information or obtaining from them genuine consent.[61]

The desire for property-like control over health data is not unique to the United States. In Europe, signs of data propertization have existed for some time in certain countries, particularly in the context of biobanking.[62] However, the recently-enacted EU-wide General Data Protection Regulation (GDPR)[63] has received the most attention in this regard.[64] As in the United States, the ability to process personal data

60. After all, these exceptions did little to rebut the claims in the *Beleno* and *Havasupai* cases. *See also* I. Glenn Cohen & Michelle M. Mello, *HIPAA and Protecting Health Information in the 21st Century*, 320 J. AM. MED. ASS'N. 231, 231 (2018) (identifying shortcomings in protections offered by HIPAA); Contreras, *Genetic Property, supra* note 15, at 33-34 (discussing gaps in regulatory exceptions for data-based research). *See also* Lisa M. Austin & David Lie, *Safe Sharing Sites,* 94 N.Y.U. L. REV. (forthcoming 2019) ("[s]trategies to mitigate the risks of re-identification affect the accuracy of the data").

61. *See* Purtova, *supra* note 30, at 219; Barbara A. Koenig, *Have We Asked Too Much of Consent?* 44 HASTINGS CENT. REP. 33, 33 (2014) ("mounting evidence suggests the distance between the ideal of consent and its actual practice"); Patrick Taylor, *When Consent Gets in the Way*, 456 NATURE 32, 32 (2008); Howard Brody, *Transparency: Informed Consent in Primary Care*, 19 HASTINGS CTR. REP. 5, 5 (1989) ("Physicians may also view informed consent as an empty charade, since they are confident in their abilities to manipulate consent by how they discuss or divulge information.").

62. *See, e.g.,* Luca Marelli & Guiseppe Testa, *Scrutinizing the EU General Data Protection Regulation: How Will New Decentralized Governance Impact Research*? 360 SCIENCE 496, 498 (2018) (discussing the Italian Data Protection Authority's decision to block the acquisition of an Italian health and genomic database by a UK firm and subsequent reversal of this decision by an Italian court); Kish & Topol, *Unpatients, supra* note 3, at 924 (describing Swiss Healthbank which "empowers users to store, manage, share and benefit from their personal health information" and "has the intent to create a global data transaction platform to support medical research").

63. GDPR, *supra* note 29.

64. The GDPR has shifted European privacy regulation from a centralized approval-based system dominated by national data protection authorities to a decentralized system in which responsibility for data protection is placed on data users and the determination of authorized users devolves to individual data subjects. *See* Marelli & Testa, *supra* note 62, at 496.

under the GDRP is based on individual consent, a concept that has, for many of the reasons cited in the United States, been subject to criticism.[65] The GDPR appears to give researchers the ability to rely on broad, non-specific consent when "keeping with recognised ethical standards for scientific research,"[66] though subsequent interpretive guidance may retreat from this position.[67] As in the United States, it is unclear what may or may not be permitted under EU regulations concerning informed consent,[68] potentially leading risk-averse institutions to follow the most conservative approach, thereby perpetuating and extending existing tendencies toward data propertization.

C. Consequences of the Propertization of Health Data

Numerous commentators have cautioned against the recognition of property-like interests in human health information on grounds both

See also Purtova, *supra* note 30, at 211 (discussing property-like interests arising from GDPR right to data portability).

65. *See* Marelli & Testa, *supra* note 62, at 496 ("the inherently open-ended potential of data, whose digital compatibility makes them valuable for research pursuits that may be wholly disjoined from the original project within which samples or data were gathered, thus undermining the classical rationale for 'informed consent.'"); Purtova, *supra* note 30, at 216.

66. GDPR, *supra* note 29, at Recital 33.

67. *See generally,* GUIDELINES ON CONSENT UNDER REGULATION 2016/679, ARTICLE 29 WORKING PARTY, *available at* http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615239 (last visited Mar. 2, 2019) (cited and discussed in Marelli & Testa, *supra* note 62, at 497) (establishing narrower guidelines in regard to giving and receiving consent).

68. *See* Marelli & Testa, *supra* note 62, at 497 (noting that reconsideration of Italian database transfer case, discussed *supra* note 62, under the GDPR will shape future interpretation of consent requirement for data research).

moral[69] and doctrinal.[70] The motivating force behind this article, however, is the practical impact that propertization may have on the conduct of biomedical research and public health monitoring. This impact flows largely from the traditional common law attributes of property: principally the right of a property owner to exclude others from intruding on that property, as well as the rights of a property owner to limit use of, or even destroy, that property and to choose to alienate and profit from the transfer of that property.[71]

Our primary concern is that the recognition of a property interest in individual health data could disrupt data-driven research if individuals have the right to withhold, recall, constrain, or destroy data after it enters the research pool.[72] As noted above, this right was claimed

69. *See, e.g.*, Angrist, *supra* note 3, at 45 (quoting bioethicist Hank Greely, "Owning kidneys makes people think of slavery. They think it degrades humanity"); Baron, *supra* note 16, at 381-90 (property law concepts such as alienability and in rem treatment are difficult to translate to the realm of personal health data); Sonia M. Suter, *Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy*, 72 GEO. WASH. L. REV. 737, 798–811 (2004) (claiming that certain things such as human tissue should never be alienable on dignitary grounds); Margaret Jane Radin, *Market-Inalienability*, 100 HARV. L. REV. 1849 (1987) (certain things should not be subject to market transactions). *Cf.* Marc Rodwin, *The Case for Public Ownership of Patient Data*, 302 J. AM. MED. ASS'N. 86 (2009) (arguing against *corporate* ownership of patient data on moral and practical grounds).

70. *See, e.g.,* I. Glenn Cohen, *Is There a Duty to Share Healthcare Data?*, *in* BIG DATA, HEALTH LAW, AND BIOETHICS 209, 212-14 (I. Glenn Cohen et al. eds., 2018) (refuting Lockean arguments for property in health data) [hereinafter Cohen, *Duty to Share*]; Barbara J. Evans, *Barbarians at the Gate: Consumer-Driven Health Data Commons and the Transformation of Citizen Science*, 42 AM. J. L. & MED. 651, 657 (2016) (arguing that many protections sought to be achieved through property law already exist in the regulatory frameworks that govern medical records and research); Barbara J. Evans, *Would Patient Ownership of Health Data Improve Confidentiality?*, 14 AM. MED. ASS'N J. ETHICS 724, 728 (2012) ("There are few discernible differences between the level of confidentiality patients would enjoy if they owned their data and biospecimens and what they presently have under the HIPAA Privacy Rule and the Common Rule.").

71. As famously described by Sir William Blackstone, property is "that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe." SIR WILLIAM BLACKSTONE, KNT., COMMENTARIES ON THE LAWS OF ENGLAND 393 (1893).

72. *See* Wolf, *supra* note 45, at 142 (arguing that the right to withdraw from a research study entails the right to prevent further use of data); Amy L. McGuire & Laura M. Beskow, *Informed Consent in Genomics and Genetic Research*, 11 ANN. REV. GENOMICS & HUMAN GENETICS 361, 370 (2010) (suggesting that research subjects that withdraw from studies be permitted to require that repositories discontinue use of personal data).

by the plaintiffs in the *Beleno* and *Havasupai* cases.[73] Yet data-driven biomedical research depends on the existence of a stable and accessible data resource. For example, large-scale studies such as All of Us by the NIH plan to enroll and collect data from up to a million individuals.[74] In order to make the greatest use of this data resource, researchers from around the world will need to access, recombine, search, and manipulate this data in whatever manner is most promising.[75] In the words of Francis Collins, Director of the National Institutes of Health, and Harold Varmus, Director of the National Cancer Institute, this flexibility is required "so that the world's brightest scientific and clinical minds can contribute insights and analysis."[76]

In the world of global data sharing, the number of researchers requiring access to a particular data element, and the specific research questions that they will seek to answer, cannot be known at the time that data is collected or consent to research is given. Thus, there is a risk that consent that is too broad or non-specific could, upon later examination, be deemed inadequate.[77] And if so, the retroactive withdrawal or destruction of individual data already incorporated into large data pools and analyses could severely compromise and/or bias such studies.[78]

What's more, a requirement that researchers obtain consent from every individual data subject prior to the commencement of research using data obtained from that individual (i.e., *ex ante*) will impose a substantial up-front burden on any sizable research program.[79] The Institute of Medicine has cited several studies showing that compliance

73. *Supra* notes 39, 45 and accompanying text.

74. *About the All of Us Research Program,* NAT'L INST. HEALTH, https://allofus.nih.gov/ (last visited Mar. 18, 2019).

75. *See* Francis S. Collins & Harold Varmus, *A New Initiative on Precision Medicine*, 372 NEW ENGL. J. MED. 793, 794-95 (2015) ("Qualified researchers from many organizations will, with appropriate protection of patient confidentiality, have access to the cohort's data").

76. *Id.* at 795.

77. This claim was made by the Havasupai in their litigation against ASU. *See* Havasupai Tribe v. Ariz. Bd. of Regents, 204 P.3d 1063, 1066 (Ariz. Ct. App. 2008). *See also* Marelli & Testa, *supra* note 62, at 497 (discussing validity of broad consent under GDPR).

78. *See* Contreras, *Genetic Property, supra* note 15, at 30 ("data and study results become skewed toward those individuals who are most willing to consent to research, whereas individuals who are less willing to consent are underrepresented"). *See also* OECD, DATA-DRIVEN INNOVATION 196-97 (2015) (identifying practical difficulties potentially arising from individual data ownership).

79. *See, e.g.*, Rumbold & Pierscionek, *supra* note 28, at 586 ("Patient 'ownership' of data would have the potential to make access to aggregated data more difficult and thus to hinder research").

with extensive data privacy and consent procedures has increased both the difficulty of recruiting study subjects and the overall cost of biomedical research.[80] And, given the way that healthcare markets work, this cost would likely be passed along to the consumer.[81]

The implications of data ownership on public health monitoring and intervention is equally troubling. Today, primary healthcare providers and emergency care centers can, and in many cases are required to, report data regarding symptoms pointing to potential disease outbreaks to public health officials.[82] This reporting may include data regarding individuals exhibiting such symptoms. Public health officials can use this data to track potential outbreaks, to implement containment strategies and to develop diagnostic tools and vaccines.[83] Obtaining individual consent to the use of data in each of these critical public health functions could severely impede the protection of public health.[84]

The fragmentation of individual ownership interests in a large resource pool can give rise to what theorists have termed an "anticommons," a situation in which progress is impeded due to the significant transaction costs required to assemble rights from multiple holders. The threat of anticommons in biomedical research was originally identified with the proliferation of patents covering genetic discoveries,[85] but has recently been raised in connection with the broadly disaggregated ownership of individual health data.[86] Such an

80. INST. MED., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 218-20 (Sharyl J. Nass et al., eds., 2009). *See also* Cohen, *Duty to Share*, *supra* note 70, at 215-16 (noting cost estimates).

81. *See* J. Cohen, *Examined Lives, supra* note 32, at 1388 ("data privacy opponents argue that increased protection would impose unreasonable costs on routine consumer transactions—costs that consumers themselves ultimately will have to bear").

82. Richard N. Danila et al., *Legal Authority for Infectious Disease Reporting in the United States: Case Study of the 2009 H1N1 Influenza Pandemic*, 105(1) AM. J. PUB. HEALTH 13, 14 (2015); *see, e.g.*, UTAH CODE ANN. § 26-6-6(1) (LexisNexis 2019).

83. Ruth Ann Jajosky & Samuel L Groseclose, *Evaluation of Reporting Timeliness of Public Health Surveillance Systems for Infectious Diseases*, BMC PUB. HEALTH 2 (2004) ("Reasons for conducting public health surveillance can include the need to assess the health status of a population, establish public health priorities, and reduce the burden of disease in a population by appropriately targeting effective disease prevention and control activities").

84. *See* Mark Rodwin, *Patient Data: Property, Privacy & the Public Interest*, 36 AM. J. L. & MED. 586, 589 (2010).

85. Michael A. Heller & Rebecca S. Eisenberg, *Can Patents Deter Innovation? The Anticommons in Biomedical Research*, 280 SCIENCE 698, 698 (1998).

86. *See, e.g.,* Jorge L. Contreras, *The Anticommons at 20: Concerns for Research Continue*, 361 SCIENCE 335, 337 (2018); Contreras, *Genetic*

anticommons, if it materializes, can significantly impede efficient transactions and thwart socially-beneficial activity.

For all of these reasons, individual property-like entitlements in health data, whether imposed through the mechanism of informed consent or otherwise, have the potential both to disrupt and substantially increase the cost of socially beneficial biomedical research. As the federal district court predicted in *Greenberg*, the recognition of individual property rights in health data could "cripple medical research."[87]

II. LIABILITY AND REGULATORY RULES FOR HEALTH DATA

Given the potential research challenges that could emerge as a result of widespread recognition of property interests in personal health data, it is worth considering whether there is an alternative framework for managing individual privacy and related interests while at the same time maximizing social welfare from biomedical research. As noted above, a useful analytical starting point for analyzing this question is offered by Calabresi and Melamed, who first drew the important distinction between property rules and liability rules in the allocation of entitlements between parties.[88]

A. Efficiency and Ex Ante versus Ex Post Systems

Under the Calabresi and Melamed framework, the initial allocation of entitlements and the choice of property versus liability rules has both efficiency, distributive, and justice-based consequences.[89] We deal first

Property, supra note 15, at 7 (anticommons in genetic information); Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 4 ("Each individual has an incentive to remove her data from the commons to avoid remote risks of re-identification. This way she gets the best of both worlds: her data is safe, and she also receives the indirect benefits of helpful health and policy research performed on the rest of the data left in the commons. However, the collective benefits derived from the data commons will rapidly degenerate if data subjects opt out to protect themselves"). Rodwin, *supra* note 84, at 606 ("private ownership of patient data would probably preclude its most valuable uses by fracturing population data"); Richard A. Spinello, *Property Rights in Genetic Information*, 6 ETHICS & INFO. TECH. 29, 35 (2004) (fragmented property rights in the genetic data coming from multiple sources would require a substantial integration effort if that data were needed for a particular research project). Somewhat counterintuitively, Kish and Topol use the "tragedy of the commons" to support their argument for individual ownership of health information. Kish & Topol, *Unpatients, supra* note 3, at 923.

87. Greenberg v. Miami Children's Hosp. Research Inst., Inc., 264 F. Supp. 2d 1064, 1076 (S.D. Fla. 2003).

88. *See* Calabresi & Melamed, *supra* note 7, at 1090.

89. *See* i*d.* at 1093-1105.

with administrative efficiency.[90] If, in a property rule regime, an entitlement is initially allocated to the occupant of land, then a traveler wishing to cross over than land must first obtain (and possibly pay for) permission to cross.[91] This *ex ante* requirement imposes an administrative burden on each act of crossing over land: permission must be sought and the right of passage must be negotiated in 100% of cases. In a liability rule regime, however, the traveler may access the land, but may later be sued for damages by the occupier.[92]

Coase tells us that, absent transaction costs, the land will either be crossed or not crossed, no matter where the initial entitlements are placed, depending on whether the occupier values her privacy more than the traveler values that particular route across the countryside.[93] That is, in either case an appropriate exchange of value will be negotiated to enable the efficient outcome to occur. But, in reality, a number of factors conspire to tilt the balance in one direction or another. Thus, in the example of the traveler, it is likely that only a subset of occupiers will seek *ex post* to recover the remedy to which they are entitled (i.e., if the traveler is not detected or does not damage the land, or if the cost of enforcing rights exceeds the occupier's predicted recovery, or if the traveler is a vagabond who would lack the resources to satisfy any judgment against him).

A similar logic holds when the initial entitlement is placed with the traveler, giving him an affirmative right to cross land occupied by someone else. Under a property rule regime, the traveler, knowing his desired route, may obtain a series of *ex ante* injunctive orders prohibiting the occupier of each tract along the route from erecting a fence blocking the route.[94] This exercise, while guaranteed to assure the traveler the ability to cross the countryside unimpeded, is likely to be time consuming and costly. In a liability rule regime, the traveler proceeds across the countryside, and if he encounters a fence erected by

90. Administrative efficiency refers to reducing the administrative costs of enforcement. *See id.* at 1093. Administrative efficiency is one component of the larger concept of economic efficiency, also known as Pareto-optimality, in which allocation choices "lead to that allocation of resources which could not be improved in the sense that a further change would not so improve the condition of those who gained by it that they could compensate those who lost from it and still be better off than before". *Id.* at 1094. As an analysis of Pareto-optimality is beyond the scope of this article, we limit our discussion of efficiency to administrative efficiency.

91. *See id.* at 1091.

92. *See id.* at 1092.

93. Ronald H. Coase, *The Problem of Social Cost*, 3 J. L. & ECON. 1, 15 (1960) (discussed in Calabresi & Melamed, *supra* note 7, at 1094 n.12 and accompanying text).

94. This exercise resembles the acquisition by eminent domain of "rights of way" by railroad and telegraph companies across large stretches of the American west.

an occupier, he may sue the occupier for damages. Assuming that occupiers of land understand that they will be liable for damages if they erect fences across a traveler's route, then only occupiers who place a value on their privacy in excess of the level of damages will erect fences. In a property rule regime, these are the occupiers that would have successfully bargained with the traveler, paying him to take an alternate route to avoid crossing their land.

The question which of these approaches – property or liability – is more efficient depends on a range of factors including the cost of fences and the ease of getting around them. If there are few occupiers willing to erect fences in the face of a damages lawsuit, then the liability regime will be more efficient than obtaining pre-clearance to cross each parcel along the desired route. But if fences are likely to pop up across every parcel along the route, then the traveler would be better off, and efficiency would be served, by obtaining an *ex ante* injunctive order to cross each parcel rather than litigating against the builder of each fence *ex post*.

Table 1 below summarizes the options available for the allocation of entitlements and remedies under the Melamed and Calabresi framework using our stylized example of an occupier of land and a traveler who wishes to traverse that land.[95]

Table 1
Calabresi and Melamed – Entitlements under Property and Liability Rules

	Type of Rule	
Entitlement in:	**Property (*Ex ante*)**	**Liability (*Ex Post*)**
Occupier	Injunction (Occupier can prevent access)	Damages (Traveler pays to access)
Traveler	Injunction (Traveler can force access)	Damages (Occupier pays if it prevents access)

B. Distributional Effects

As observed by Calabresi and Melamed, "the placement of entitlements has a fundamental effect on a society's distribution of wealth."[96] Distributional effects can arise both from the choice of initial entitlements and the choice between property and liability regimes. In the scenario described above, if initial entitlements are placed with land occupiers, then under a property rule regime, an occupier who values her privacy can prevent a traveler from crossing her land at no cost. If a traveler wishes to cross, he would have to pay her the value that she places on her privacy, say $5. In a liability rule regime, if a traveler crosses her land without permission, then she can recover that $5 in

95. *See* Calabresi & Melamed, *supra* note 7, at 1115-16.

96. *Id.* at 1098.

damages from him. If, however, initial entitlements are placed with travelers, then in a property rule regime, the occupier would have to pay the traveler to refrain from crossing her land at the value he places on making the crossing (say $7). Likewise, if she erects a fence under a liability rule regime, the traveler can recover damages from her (also $7). Thus, depending on the initial allocation of entitlements, and absent transaction costs, in order to prevent the traveler from crossing her land, the occupier will either spend $0 or $7. The converse holds true for the traveler if he wishes to cross against the will of the occupier. The placement of initial entitlements thus has a clear distributional effect, even if it does not impact the ultimate use of a particular asset.

In addition to the straightforward distributional effects arising from placement of entitlements, transaction costs play a large role in skewing the distribution of wealth. Thus, it is well-known that the cost of enforcing rights can be significant, and that large enterprises are more likely and able to enforce their rights in court than individuals. Likewise, the cost of monitoring compliance with legal rules can be significant, and larger organizations are often better placed than individuals to effectively monitor compliance. As a result, parties that are less able and willing to assert their rights will often forego remedies that might otherwise be available to them.

Finally, it is important to note that, despite the stylized analysis common to discussions of property and liability rules, the "damages" available to an entitlement holder under a liability rule framework will not necessarily reflect actual harm or injury to the entitlement holder, or the value that either party places on the activity in question. Rather, for purposes of administrability and uniformity, the amounts levied on parties in liability rule regimes may be fixed by the state in a manner that does not take into account the particular preferences or circumstances of the parties at all. Speeding fines, for example, are fixed by the state without regard to the driver's wealth, ability to pay, or the urgency of his need to get to his destination. With respect to intellectual property, an example can be found in the compulsory licensing scheme for musical compositions under the U.S. Copyright Act.[97] Under this framework, the copyright in a composition (the entitlement) resides with the composer, yet any person wishing to make a recording of the composition after the initial recording is released (i.e., a cover or remake version) may do so without the copyright owner's permission upon payment of a royalty fixed by the governmental Copyright Royalty Board.[98] And in some cases, such user privileges (as in the case of fair

97. 17 U.S.C. § 115 (2016).

98. 17 U.S.C. § 801(a) (2018).

use under the Copyright Act[99]) may be granted against an entitlement with no monetary compensation whatsoever.[100]

C. Justice and Social Welfare

Calabresi and Melamed observe that "those preferences which cannot be easily explained in terms of [a] few broadly accepted distributional preferences, or in terms of efficiency, are termed justice reasons."[101] Yet, Calabresi and Melamed appear uncomfortable with the notion of justice. They explain, in economic terms, that most social preferences, even seemingly non-quantitative values such as equality, can be grounded in distributional preferences or efficiency motivations or both.[102] They thus cut short their discussion of justice without offering tangible examples of those "idiosyncratic" values that cannot be placed within the rubrics of either distribution or efficiency.[103]

We do not share this seeming discomfort with the notion of justice. Clearly, in the area of human subjects research, considerations of individual autonomy, choice, privacy, and dignity are important. Likewise, where research using individual health data is concerned, these considerations must be taken into account, for reasons of fairness and justice, if nothing else.

Though important, we do not view these considerations as pre-empting all others. Social welfare (e.g., identifying risk factors and finding new cures for disease), which sounds in economic efficiency and distributional concerns, is also important. And, in some cases, the promotion of social welfare can outweigh an absolutist deference to individual choice. Some commentators, in fact, speak of an individual ethical obligation, grounded in principles of beneficence and justice, to help others by participating in socially beneficial research.[104] As explained by Patrick Taylor,

---

99. 17 U.S.C. § 107 (1992).

100. *See* Dan L. Burk, *Critical Analysis: Property Rules, Liability Rules and Molecular Futures – Bargaining in the Shadow of the Cathedral*, *in* GENE PATENTS AND COLLABORATIVE LICENSING MODELS 294, 301 (Geertrui van Overwalle, ed., 2009).

101. Calabresi & Melamed, *supra* note 7, at 1105.

102. *Id.*

103. *Id.*

104. *See* Cohen, *Duty to Share, supra* note 70, at 216-18 (discussing arguments by Alan Wertheimer and others regarding a moral duty to participate in research); Brent Mittelstadt et al., *Is There a Duty to Participate in Digital Epidemiology?* 14 LIFE SCI., SOC'Y & POL'Y 1, 4-5 (2018) (summarizing justifications for a "moral duty for patients to contribute to biomedical research," including arguments grounded in beneficence, avoidance of free riding, public goods and solidarity); David Orentlicher, *Making Research a Requirement of Treatment – Why We Should Sometimes Let Doctors Pressure Patients to Participate in Research*, 35 HASTINGS CTR. REP. 20, 21 (2005) ("linking treatment to participation in

> An enduring ethical position is that we should reciprocate in social arrangements through which we ourselves benefit, when the duties are fairly distributed across society. A good example is improvement to health-care quality, for which access to all patient outcomes is critical. Risks from participation are low, and benefits to all are high. We depend on participation, and share a duty to participate in return. We cannot simply demand the benefit and decline the cost.[105]

We, too, believe that promoting biomedical discovery to improve overall human health is an important social goal that should be set aside only for reasons recognized as highly compromising or injurious to individuals. For example, if a researcher wished to publish the names and street addresses of participants in a mental health study so as to "personalize" his results for a magazine article, considerations of individual privacy should clearly override any marginal benefit that such disclosure might achieve. By the same token, if an individual who participated in a genetic study bore a personal animus toward members of a different ethnic group and wished to allow the use of her anonymized data for research concerning diseases affecting her own ethnicity, but not those primarily affecting the other ethnic group, there would be few legitimate reasons that such a request should be honored, notwithstanding the entitlement holder's personal preference. Thus, while important, personal autonomy cannot override the broader needs of society.[106] In our proposals below, we seek to promote a system that appropriately balances interests of personal privacy, autonomy, and self-determination with broader considerations of social welfare.

D. Entitlements and the Role of the State

As initially formulated by Calabresi and Melamed, initial entitlements are set by the state within a framework in which enforcement mechanisms are enabled by the state's authority.[107] Thus, the state provides a judicial system that adjudicates and enforces judgments awarded to private parties, but the responsibility for monitoring compliance with entitlement rules and bringing actions to enforce them rests with those private parties. Likewise, when a party brings an action seeking damages against another party (e.g., for trespass), those damages are paid to the aggrieved party and are not remitted to the state, even though the state's authority enables the

---

research could be a valuable and ethically sound way to increase patient participation, as long as the clinical trial involves a comparison of alternative, established therapies").

105. Taylor, *supra* note 61, at 32.

106. *See id.* at 33 ("If we protect privacy effectively, we will not reduce ethics to autonomy, and autonomy to data ownership.").

107. Calabresi & Melamed, *supra* note 7, at 1090-91.

aggrieved party to enforce its judgment against the liable party. In this framework, the state acts largely in the background and is not itself a principal actor, except as the setter of rules and allocator of initial entitlements.

It is often the case, however, that the state intervenes more directly in the monitoring and enforcement of non-compliance with conditions imposed on those entitlements. As conceptualized by Henry Smith, a more finely-grained determination of permitted and prohibited activities involving an entitlement is sometimes preferable to the broad-brushed right to exclude that traditionally accompanies property rights.[108] This "governance" approach lends itself to governmental regulation rather than private enforcement of rights. For example, the state may grant an entitlement, such as the right to build a power plant, that is conditioned on the *ex ante* payment of a permitting fee to the state.[109] The state may also impose *ex ante* licensure and approval requirements before some activity is undertaken (e.g., a requirement that a safety inspection be passed, or that drivers pass written tests and vision exams before being permitted to drive on public roads).[110]

The state may also impose *ex post* fines and penalties when private behavior violates rules or regulations.[111] For example, parking on the public streets of a densely-populated neighborhood can be restricted to those displaying a residential parking permit. When a non-resident illegally parks on the street, making it more difficult for residents to find parking, private litigation by affected residents may not be efficient. Instead, the city issues a ticket and fine to the offender and, under some circumstances, tows the offending car away. The remedies available to the state can be exercised both speedily and objectively, in a manner much more effective than private litigation by aggrieved residents. However, when a parking ticket is issued, the fine is paid to the state, not to the aggrieved residents. The benefit they receive is not a share of the parking fine, but the improved enjoyment of their parking entitlement which is made possible through the state's enforcement mechanisms.

The remedial options available to the state when it intervenes to protect entitlements differ structurally from the options available to individuals making use of the legal system in order to obtain injunctions or seek damages. Shavell illustrates the different remedial options available to individuals and to the state in the context of risk regulation in *Table 2* below.[112]

---

108. Henry E. Smith, *Exclusion versus Governance: Two Strategies for Delineating Property Rights*, 31 J. LEG. STUD. S453, S454-55 (2002).

109. *See, e.g.*, Calabresi & Melamed, *supra* note 7, at 1099.

110. *Id.*

111. SHAVELL, *supra* note 11, at 278.

112. *Id.*

Table 2
Shavell – Ex ante and Ex post remedies for risk control

	When applied	
How initiated	***Ex ante***	***Ex post***
Privately initiated	Injunction (against risky behavior)	Liability (for harm caused by risky behavior)
State initiated	Corrective tax (to compensate society for likely harms from risky behavior) Safety regulation (to ensure that planned behavior is within acceptable safety limits)	Fine for harm caused by risky behavior

As explained by Shavell, in the context of different types of risk avoidance, there may be advantages to giving remedies, and the principal responsibility for policing behavior, to the state.[113] For example, the state may be a more effective *ex ante* judge than individuals whether a particular activity (e.g., constructing a building) meets acceptable safety levels (e.g., building codes). It may also impose conditions, such as training and licensure of new drivers, on the conduct of risky activity. Likewise, *ex post*, it may be more efficient for the state to conduct building inspections and levy fines and corrective penalties against builders that do not meet code than to rely on individuals discovering such violations and bringing private enforcement actions. If society's goal is to detect as many safety risks as possible, then relying on the state rather than individuals may be preferable. And from the standpoint of remedies, paying an *ex post* fine to the state, which may support the state's monitoring and inspection functions, may be more socially valuable than permitting individuals to seek and collect windfall monetary damages. The state, which can be deemed to act on behalf of its citizens, can thus be considered as a proxy for its citizens in terms of collection of damages affecting society broadly.

In addition to which party is the more efficient policer of activity and recipient of damages (the individual or the state), Shavell asks whether *ex ante* or *ex post* remedies are more likely to achieve desired social outcomes.[114] One consideration, for example, is whether a violator would generally have the ability to pay *ex post* damages for harm that it caused. If, on balance, it would not (either because violators have few assets or because likely harms are very large - e.g., nuclear plant disasters), then *ex ante* charges and inspections prior to allowing risky activity might be preferred.[115]

113. *Id.* at 281-82.

114. *Id.* at 279.

115. *See id.* at 284.

Shavell also addresses those situations in which state-imposed criminal sanctions may be desirable to address non-compliance with rules associated with entitlements. In general, he concludes that criminal penalties are advisable when monetary penalties are unlikely to deter undesirable behavior (e.g., when the injurer has few assets, or has set out to do harm).[116]

E. Combining the Frameworks – Entitlements and Health Information

When considering the optimal framework for governing research using personal health information, it is useful to combine the approaches outlined by Calabresi and Melamed, with respect to initial entitlements, and that of Shavell, with respect to state versus private remedies. To simplify matters, we make the initial and, hopefully non-controversial, decision to place the initial entitlement with respect to individual health data with the individual. This placement is both intuitive and generally consistent with existing legal regimes that protect an individual's privacy in health-related data.

A second adjustment that we make to the Shavell framework is including publicly-chartered data repositories within the ambit of state (governmental) actors. These data repositories include biobanks and databases that are operated or overseen by governmental agencies, academic institutions, hospital networks, and non-profit research centers.[117] We group these organizations together with more traditional governmental agencies even though some of them are not, strictly speaking, governmental bodies, due to their overall similarity and position with respect to health data users (researchers) and individual data subjects. That is, these data repositories act as the custodians of individual data under a relationship of trust and stewardship and conduct their operations in the public interest, along with other governmental regulatory and enforcement bodies. We thus treat them together.

Third, in the area of remedies, we distinguish between penalties imposed on individual researchers and on the institutions that employ them. This differentiation allows graduation of penalties based on severity and prevalence within an institution. In addition, imposing penalties at an institutional level may create strong incentives within institutions to educate individual researchers regarding the relevant rules and restrictions concerning individual data usage, to monitor

116. *Id.* at 284-85.

117. For a discussion of state-operated genomic data repositories such as GenBank and the Database of Genotypes and Phenotypes (dbGaP), *see* Jorge L. Contreras, *Leviathan in the Commons: Biomedical Data and the State in* GOVERNING MEDICAL KNOWLEDGE COMMONS 19, 27-28 (Katherine J. Strandburg et al., eds., 2017) [hereinafter Contreras, *Biomedical Data*].

research compliance with those rules and restrictions, and to mitigate any violations that are discovered at an early stage.

Given these considerations, *Table 3* below illustrates the relevant structural options with respect to the governance of research using human health information.

Table 3
Structural Governance Options for Health Information
(initial entitlement in data subject)

	Rule Framework		
Right to Assert	***Property (Ex ante)***	***Regulatory/Liability (Ex post)***	
Data Subject	Consent (to permit research)	Liability (monetary compensation for harm caused by research)	
Public Authority	Community engagement	Individual	Institutional
	Licensure (of researchers)	Debarment	Debarment
		Remediation (data removal, retractions)	Remediation (data removal)
		Professional sanctions	Fines and penalties
		Criminal	

1. Property Rules Enforced by Data Subjects – Consent

With the initial entitlement assigned to an individual data subject, the individual's *ex ante* consent is required in order to permit data-based research. This scenario is akin to that of the traveler requiring *ex ante* permission from each land occupier to cross their land. As discussed elsewhere, there are serious doubts concerning the legitimacy and validity of individual consent in the healthcare setting, at least in the manner in which consent is sought and obtained today.[118] And as discussed in Section I.C above, a property rule system requiring advance consent from every data subject imposes significant costs and delays on socially valuable research programs, particularly when they involve thousands or millions of individuals, and can also result in the compromise of data sets and analysis. For all of these reasons, we do not recommend this approach.

2. Property Rules Enforced by the State – Consultation and Licensure

In a system in which the state acts as the representative or proxy for individuals, the state may "consent" to the use of individual health data subject to certain conditions. In a property rule (*ex ante*) regime, this advance authorization may be conditioned upon the satisfaction of certain criteria, which might include outreach to and engagement with

118. *See supra* note 61 and accompanying text.

relevant communities and community leaders, as well as adequate training and licensure of researchers.

The engagement of researchers with patient advocacy groups has shown particular promise with closely knit disease-specific communities[119] and minority or disadvantaged groups.[120] We support inclusive outreach measures along these lines. However, we do not believe that these forms of patient engagement and outreach need to be mandated by property rules, and also suspect that advocates of individual consent would find such approaches, standing alone, to be inadequate.

Likewise, requirements such as training and licensure of researchers regarding proper research usage of individual data seems to be a necessary but insufficient measure. Regular training of all members of a research team engaged in human subjects research is already required by the U.S. National Institutes of Health for all NIH-funded studies,[121] and should continue to be required. But, as the example of traffic violations illustrates, driver training and licensure alone are seldom sufficient to ensure compliance with applicable rules.

3. Liability Rules Enforced by Individuals - Compensatory Damages

In the realm of liability rules, individual entitlement holders may sue unauthorized infringers on their entitlements for monetary damages. Thus, just as a property occupier may sue an unauthorized trespasser for compensatory damages, an individual could sue an unauthorized user of her personal health data.

Numerous existing private causes of action may already be brought with respect to the misuse of personal data, many of which can result in an award of monetary damages to the injured data subject. Damages in such cases may be compensatory and may also reflect a punitive or

119. *See, e.g.*, Sharon F. Terry et al., *Science and Society: Advocacy Groups as Research Organizations: The PXE International Example*, 8 NATURE REV. GENETICS 157 (2007) (detailing interaction between researchers and gene-specific disease advocacy communities); Knoppers, supra note 35, at 213 (noting HUGO support for "prior discussion and consultation with communities and populations"). *Cf.* Lee A. Bygrave & Dag Wiese Schartum, *Consent, Proportionality, and Collective Power, in* REINVENTING DATA PROTECTION 157 (Serge Gutwirth, et al., eds., 2009) (introducing concept of collective consent).

120. *See, e.g.*, James V. Lavery, *Building an Evidence Base for Stakeholder Engagement*, 361 SCIENCE 554 (2018) (citing, among other examples, outreach to the Havasupai community).

121. Required Educ. in the Protection of Human Res. Participants, Notice OD-00-039, Natl. Inst. Health (June 5, 2000), https://grants.nih.gov/grants/guide/notice-files/not-od-00-039.html.

exemplary character.[122] For example, the U.S. Genetic Information Nondiscrimination Act (GINA) prohibits discrimination by employers and health insurers on the basis of an individual's genetic information.[123] The conduct prohibited by GINA is far-reaching, as the statute bars even the collection of employee genetic information by an employer.[124] Employment-based actions under GINA are filed by aggrieved employees with the Equal Employment Opportunity Commission (EEOC), and then advance through an administrative process which is subject to appeal to the courts.[125] The largest GINA verdict of which we are aware was an award of $2.2 million to two employees of a company that sought to collect DNA samples from them while investigating the vandalism of one of its warehouses.[126]

Other causes of action may give an individual a monetary remedy when data about the individual is used in a manner to which he or she has not consented. These include common law actions for violation of privacy, deceit, fraud, deception, and breach of fiduciary duty (usually brought in the context of a healthcare provider).[127] In the famous *Moore*

122. In a recent article, Lauren Scholz argues that restitution is the proper measure of privacy damages. Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L. REV. 1,1 (2018).

123. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-223, 122 Stat. 881 (2008) (codified as amended in scattered sections of 29 and 42 U.S.C.) [hereinafter GINA]. For a general discussion of GINA and an assessment of its first ten years in force, see Bradley A. Arehardt & Jessica L. Roberts, *GINA, Big Data, and the Future of Employee Privacy*, 128 YALE L.J. (forthcoming 2019); Barbara J. Evans, *The Genetic Information Nondiscrimination Act at Age 10: GINA's Controversial Assertion that Data Transparency Protects Privacy and Civil Rights*, 60 WM. & MARY L. REV. (forthcoming 2019); Contreras, *Genetic Property, supra* note 15, at 41-43 (discussing liability rule framework under GINA). Protections such as those offered by GINA are not unique to the United States. Aime Keis, *Biobanking in Estonia*, J.L. MED. & ETHICS 20, 22 (2016) (Estonian law "prohibits discrimination and stigmatization of gene donors" and "[p]roviding any [genetic] information to insurance companies or employers").

124. GINA, Sec. 202(b).

125. *See* GINA 42 U.S.C. § 2000e-16 (2015).

126. Lowe v. Atlas Logistics Grp. Retail Serv. (Atlanta), LLC, 102 F. Supp. 3d 1360, 1361 (N.D. Ga. 2015) (the vandalism included the placement of human feces in one of the company's warehouses, which the company sought to identify by matching it to the DNA of its employees).

127. For a more detailed discussion of these causes of action, see Contreras, *Genetic Property, supra* note 15, at 51-53. Jack Balkin has introduced the idea of an information fiduciary, "a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship." Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1209 (2016). This concept appears well-suited to frame private actions and liability for health data breaches.

case, even though Mr. Moore's property law conversion claim failed, he succeeded in his tort and fiduciary claims against UCLA and its physicians.[128]

We support the use of *ex post* liability rules such as these to govern the use of individual health data. However, we feel that liability rules based on individual enforcement are insufficient. As noted above, individuals often lack the expertise, resources, and information necessary to monitor and police behavior of data users.[129] Moreover, U.S. tort law does not offer particularly generous remedies for purely dignitary harms,[130] and, as noted by Litman in questioning the effectiveness of tort law for regulating data privacy, "common law lawmaking is ordinarily both gradual and slow."[131] Accordingly, we would reserve individual-based actions to those that are likely to have a significant and particularized impact on the individual's personal or financial condition. For more diffuse and generalized harms, we recommend actions initiated by public authorities, as described below.[132]

4. Rules Enforced by Public Authorities – Institutional and Professional Penalties

As summarized in *Table 3*, in addition to injured individuals, data repositories and governmental agencies (public authorities) may bring actions to enforce data usage rules. The policing of data usage by public authorities in the area of healthcare is far from new. Federal rules governing the appropriate usage of individual health data exist in both the so-called "Common Rule" that applies to all federally funded research on human subjects[133] and the HIPAA Privacy Rule.[134] Given the superior information that public authorities would likely have about

128. Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 493 (Cal. 1990); *see also* Litman, *supra* note 32, at 1308 (discussing tort and fiduciary remedies for privacy violations).

129. For a more detailed discussion of monitoring and enforcement costs in the context of genetic data regulation, see Contreras, *Genetic Property, supra* note 15, at 48-49.

130. *See, e.g.*, William L. Prosser, *Intentional Infliction of Mental Suffering: A New Tort*, 37 MICH. L. REV. 874, 877 (1939) ("If the plaintiff is to recovery every time that her feelings are hurt, we should all be in court twice a week."); Russell Fraker, *Reformulating Outrage: A Critical Analysis of the Problematic Tort of IIED*, 61 VAND. L. REV. 983, 1000-1001 (2008).

131. Litman, *supra* note 32, at 1313.

132. Litman also appears, though somewhat unenthusiastically, to support a combined tort and regulatory approach. Litman, *supra* note 32, at 1313 ("If what data privacy really needs is federal statutory protection, tort litigation is actually a plausible route to enactment").

133. General Requirements for Informed Consent, 45 C.F.R. § 46.116 (2017).

134. 45 C.F.R. § 160 (2003); 45 C.F.R. § 164 (2003).

data usage practices, as well as superior resources for monitoring compliance with data usage rules, public authorities are likely to be in a better position than affected individuals to ensure broad rule compliance and achievement of data protection and privacy goals. We thus recommend *ex post* public authority enforcement as a preferred method for regulating research using individual health information.

a. Monetary Fines and Penalties

As part of their enforcement function, public authorities may seek to impose monetary fines and penalties on violators of these rules. Such penalties are sometimes imposed today in particularly egregious cases of research misconduct.[135] The authority to impose such fines and penalties is inherent to governmental agencies but could also be authorized by contracts between data repositories and data users. The imposition of fines and penalties in the context of research misconduct has historically been rare. The possibility of such penalties, however, has become more prominent in Europe following implementation of the GDPR, which imposes substantial monetary fines for misuse of personal data,[136] and in the United States following Duke University's recent agreement to pay $112.5 million in settlement of a range of research misconduct claims.[137]

b. Remediation

In addition to monetary remedies, many cases of research misconduct involve remedies designed to reverse the harmful effects of a particular violation. Such remedies include heightened oversight,[138] retraction of published papers,[139] disgorgement of grant awards,[140] and,

135. *See, e.g.,* Greg Langlois, *Pitt Prof to Pay $132K for Science Research False Grant Claims*, BNA LIFE SCI. L. & INDUS. RPT., Mar. 23, 2018 ("University of Pittsburgh professor required to pay penalty of $132.027 for allegedly falsifying data in NSF grant applications").

136. *See, e.g.*, Marelli & Testa, *supra* note 62, at 496 (fines of up to 20 million Euros or 4% of a company's annual global revenue).

137. *See* Sheila Kaplan, *Duke University to Pay $112.5 Million to Settle Claims of Research Misconduct*, N.Y. TIMES (Mar. 25, 2019), https://www.nytimes.com/2019/03/25/science/duke-settlement-research.html.

138. *See, e.g.,* Alison McCook, *Duke's Mishandling of Misconduct Prompts New U.S. Government Grant Oversight*, SCIENCE, Mar. 23, 2018, https://www.sciencemag.org/news/2018/03/duke-s-mishandling-misconduct-prompts-new-us-government-grant-oversight (U.S. NIH imposes stringent oversight requirements on Duke University in the wake of misconduct allegations).

139. *See, e.g.*, RETRACTION WATCH, https://retractionwatch.com (last visited May 17, 2018) (cataloging retraction of scientific papers).

140. Disgorgement is a rare and severe remedy. *See* Leonid Schneider, *What if Universities Had to Agree to Refund Grants Whenever There was a*

in relation to the proposal made in this paper, the deletion of ill-gotten or misused data.

Remedies such as these are typically designed to be obtained by governmental agencies, though in the case of health information, data repositories might also be in a position to seek such remedies when authorized under applicable contractual arrangements. In the case of remediation remedies, it is important that individual data subjects *not* have the right to seek the destruction or return of data pertaining to themselves. Conceding such a right would push health information back toward a property rule regime and the welfare reducing outcomes seen in cases such as *Beleno* and *Havasupai*. Thus, the right to require deletion or destruction of health data should be used sparingly, and only against a particular data misuser, rather than the entire research community.

c. Debarment

Though imposed only occasionally, one of the most punitive remedies available in research misconduct cases is the debarment of individual researchers or, on rare occasions, institutions, from certain benefits or privileges. Typically, debarment prohibits a researcher from participating in government-funded research, or seeking further research funding, for one to three years.[141] Because of the significant impact that debarment can have on an individual's career, this remedy is sought and imposed only a handful of times per year by the major scientific funding agencies in the United States.[142] Debarment of research institutions from seeking federal grant support is largely unheard of, given the catastrophic effect that such a measure would likely have on most research institutions. However, debarment of contractors (including large firms) from seeking and obtaining government contracts is not uncommon in cases of fraud, embezzlement, unfair trade practices, failure to perform, and other inappropriate conduct.[143] Debarment remedies could also be extended to biomedical research institutions.

Retraction?, RETRACTIONWATCH (Jan. 19, 2015), https://retractionwatch.com/2015/01/19/universities-agree-refund-grants-whenever-retraction/.

141. *See, e.g.,* Jeannie Baumann, *New York University Professor Slapped with Research Debarment*, BNA LIFE SCI. L. & INDUS. RPT., Mar. 21, 2018 (reporting on a former NYU professor debarred from government-funded research for three years after allegedly falsifying images in published papers); *Findings of Research Misconduct*, NATL. INST. HEALTH (Apr. 19, 2018), https://grants.nih.gov/grants/guide/notice-files/NOT-OD-18-169.html (recounting the story of a UNC researcher debarred from federally-funded research for two years after finding of data falsification).

142. *See* Jeffrey Mervis, *After the Fall*, 354 SCIENCE 408, 409 (2016).

143. *See Frequently Asked Questions: Suspension and Debarment*, U.S. GEN. SERVICES ADMIN., https://www.gsa.gov/about-us/organization/office-of-

In the case of data misuse, debarment remedies could include blocking the access of individual researchers or institutions to some or all data. Unlike several other remedies discussed above, debarment in the case of data misuse would likely be sought by the data repository (rather than an aggrieved individual or government agency) given the repository's custodial role over such data.

d. Other Penalties

In addition to the penalties described above, research institutions may impose professional sanctions on individual researchers that violate rules regarding data access and use. These sanctions may range from minor (e.g., warnings) to severe (e.g., demotion or dismissal). While only the institution itself has the authority to impose these sanctions, either a governmental agency or a data repository may require an institution to discipline its individual researchers as part of the conditions permitting institutional access to a data resource.

Finally, it is always the case that violation of data privacy or security rules may result in civil or criminal penalties beyond what may be stipulated in a set of data access rules. Enforcement of these legal penalties is the sole province of government and should generally be reserved for violations of the most serious nature.

5. A Proposed Rule Framework for Health Information

To summarize the above, we propose that research using individual health data should be subject to a regulatory regime, enforceable by government/public repositories, while at the same time permitting limited private enforcement actions to address particularized individual injury. Thus, while the physical collection of human tissue would continue to be subject to existing rules regarding informed consent,[144] *ex ante* consent would *not* be required for the use of information derived from physical samples. Rather, rules regarding proper research use of health information would be put in place, and violations of those rules

---

governmentwide-policy/office-of-acquisition-policy/gsa-acq-policy-integrity-workforce/suspension-debarment-division/suspension-debarment/frequently-asked-questions-suspension-debarment#Q4 (last reviewed Feb. 26, 2019).

144. For example, physical DNA samples could be collected during any routine medical procedure to which the subject consented, or via a special procedure (e.g., saliva swab, blood draw) for which any physical risks were adequately disclosed and to which the subject has consented. Likewise, DNA collected through non-invasive means, such as the collection of crime scene evidence, would not trigger any consent requirement. *See, e.g.*, Rebecca Robins, *The Golden State Killer Case Was Cracked with Genealogy Website. What Does That Mean for Genetic Privacy*? STAT (Apr. 26, 2018), https://www.statnews.com/2018/04/26/genealogy-golden-state-killer-privacy/ (describing the apprehension of a notorious serial killer by combining DNA evidence with public databases, all without the consent of the suspect).

could be dealt with on an *ex post* basis. The precise conduct that these rules would cover remains open to debate, and should be discussed broadly by researchers, research funders, and patient groups. A range of commentators have proposed that data usage and privacy rules be enhanced to prevent misuse of personal data, re-identification of data subjects, insufficient data security measures, and other misuses.[145] Existing examples of data usage and protection rules are described in the case studies in Part III below.

Whatever rules are put in place, researchers who violate those rules would be subject to penalties that could include monetary damages and fines, debarment, and remedial measures. However, data would not have to be destroyed or removed from existing data sets, and permissible research using that data could continue unabated. Thus, while deterrents would exist to dissuade individual and institutional researchers from engaging in abusive practices, socially beneficial research by innocent researchers could continue unimpeded. And because *ex ante* consent from every research participant would not be required, the efficiency of the research enterprise would be improved.[146]

145. *See, e.g.* Contreras, *Genetic Property, supra* note 15, at 44-48 (proposing liability rules to enhance existing GINA protections, prohibit reidentification of data subjects, restrict commercial uses of data and enhance data security); Taylor, *supra* note 61, at 33 ("Governments should broaden privacy protections to extend across all organizations and agencies that hold sensitive information, including web service providers, pharmaceutical companies, corporate data-miners, providers of personal health records, universities and government. Reidentifiability must be addressed and prevented in cases in which extensive linkage between health and genetic information is maintained."); Cohen & Mello, *supra* note 60, at 232 (proposing "expanding the penalties and civil remedies available for data breaches and misuse, including reidentification attempts" and "a general rule protecting health data that specifies further, custodian-specific rights").

146. Overall cost savings would emerge if the cost of monitoring and enforcing noncompliance with research rules (*see* Contreras, *Letter*, *supra* note 6, at 48-50 (discussing monitoring and enforcement costs)) were lower than the cost of seeking and obtaining consent from all research participants. As such, it is likely that overall costs will be lower under a liability rule system in scenarios with large numbers of individual participants (*ex ante* consent cost) and a low incidence of noncompliance with rules (*ex post* enforcement cost). It is a separate question how these overall costs are allocated. Without state intervention, it can be assumed that *ex ante* consent costs will be borne by researchers and e*x post* monitoring and enforcement costs will be borne by individual research subjects. The state can adjust initial entitlements and burdens to reflect social priorities. For example, in the case studies described in Section II.B. below, the state itself has assumed the burden of compliance monitoring and enforcement (*see supra* note 187 and accompanying text).

III. RULES FOR HEALTH DATA RESEARCH - TWO CASE STUDIES

In this section we present two case studies – one from the United States and one from Denmark – in which governmental rules have been used successfully to govern large-scale repositories of health data. These repositories each operate under a statutory mandate independent of general rules governing human subjects research and informed consent. These case studies demonstrate that a regulatory framework, in lieu of a property rule framework, may be both practical and useful in governing research using human health data.

A. Utah Population Database (UPDB)

The Utah Population Database (UPDB) comprises a large set of linked health, genealogical and demographic records pertaining to residents of the U.S. state of Utah, their relatives, and their ancestors around the world.[147] The resource, which extends back to the late eighteenth century (seventeen generations), contains more than thirty-one million records with data from nearly ten million individuals.[148] The UPDB is unique in that it links records from three distinct types of sources: state and federal vital statistics records (birth, death, marriage, divorce, drivers' license, Social Security, and voting registration records), nearly two million multigenerational genealogical records from the Church of Jesus Christ of Latter-day Saints (the Mormon church),[149] and more than 500,000 state cancer registry records (which, in recent years, have included an increasing number of biospecimens).[150] The

147. *See generally* Ken R. Smith et al., *The Utah Population Database: A Model for Linking Medical Genealogical Records for Population Health* (forthcoming); Lisa A. Cannon Albright, *Utah Family-Based Analysis: Past, Present and Future*, 65 HUMAN HEREDITY 209, 210 (2008); Mark H. Skolnick, *The Utah Genealogical Database: A Resource for Genetic Epidemiology*, in BANBURY REPORT NO. 4: CANCER INCIDENCE IN DEFINED POPULATIONS 285, 285, 287 (John Cairns et al., eds., 1980).

148. *See* Smith et al., *supra* note 147, at 5; *Utah Population Database,* HUNTSMAN CANCER INST., https://healthcare.utah.edu/huntsmancancerinstitute/research/updb/data/ (last updated June 8, 2018) [hereinafter UPDB Data].

149. The Mormon faith places a high value on ancestral and genealogical information. As such, the Mormon church maintains what it claims to be "the largest collection of family records in the world", containing information on an estimated 3 billion living and deceased individuals from more than 100 countries. *Genealogy*, CHURCH OF JESUS CHRIST OF LATTER-DAY SAINTS, https://www.mormonnewsroom.org/topic/genealogy (last accessed Mar. 08, 2019).

150. *See* UPDB Data, *supra* note 148. Cancer registry data includes approximately 350,000 records from the Utah Cancer Registry and 200,000 records from the Idaho Cancer Registry. Cancer is a reportable

compilation and linkage of these data sets enable a range of epidemiological and genetic studies. For example, the linkage of multigenerational family genealogies with death records and cancer registry data has enabled the identification of familial patterns of cancer susceptibility across a wide range of tumor types, which can then facilitate recruitment to further studies.[151]

The state of Utah, like all U.S. states, provides for the collection of health data for statistical and public health purposes. This power is currently delegated to the Utah Department of Health, which has the authority to collect and maintain a broad range of health data.[152] Personally identifiable health data collected by the Department may not be disclosed except with the consent of the data subject[153] or under a number of statutory exceptions. One of these exceptions permits the disclosure of health data "for bona fide research and statistical purposes" as determined by the Department, provided that the recipient of the information enters into a written agreement to protect the data in accordance with legal requirements and not to permit its further disclosure.[154] The use of individual health data for research purposes is further protected under a statutory liability shield, which permits any person, without incurring liability, to provide data relating to the "condition and treatment" of an individual, as well as familial and other related information, to "scientific and health care research organizations affiliated with institutions of higher education" for the purpose of "study and advancing medical research" among other things.[155]

The linkage of Utah vital statistics records with Mormon genealogical records began in the early 1970s through a collaboration between the University of Utah and the Mormon church.[156] In 1982, Governor Scott Matheson issued an Executive Order creating the Utah Resource for Genetic and Epidemiologic Research (RGE) as a "data resource for the collection, storage, study, and dissemination of medical and related information" to be used "for the purpose of reducing morbidity or mortality, or for the purpose of evaluating and improving

---

condition in many states including Utah. UTAH ADMIN. CODE r.384-100-1 (2017).

151. *See* Smith et al, *supra* note 147, at 3, 15; Cannon Albright, *supra* note 147, at 210-218.

152. UTAH CODE ANN. § 26-3-2 (LexisNexis 2017) (enacted 1981).

153. UTAH CODE ANN. § 26-3-7(1) (LexisNexis 2017) (enacted 1981).

154. UTAH CODE ANN. § 26-3-7(3) (LexisNexis 2017) (enacted 1981). *See also* UTAH CODE ANN. § 26-3-10 (LexisNexis 2017) (enacted 1981) (pertaining to Department measures required to protect identifiable health data).

155. UTAH CODE ANN. § 26-25-1(1)-(3) (LexisNexis 2017) (enacted 1981).

156. Smith et al., *supra* note 147, at 4.

the quality of hospital and medical care."[157] The RGE was originally administered by the Utah Department of Health, but in 1986 this authority was transferred to the University of Utah,[158] which continues to oversee the UPDB today.

UPDB does not engage in primary data collection. Rather, it links data from a range of public sector and private data sources, provides front-end search and analytical capabilities, and makes these resources available to approved researchers (discussed below). Because most data linked by UPDB was not collected for research purposes, but for official governmental or church recordkeeping, the consent of individual data subjects has not been sought or obtained either by UPDB or the original data collector (e.g., church or state agencies).[159] Given this acknowledged omission, RGE is charged with safeguarding the privacy and security of individual data that is accessible through the UPDB.[160]

In order to access and use data through the UPDB, researchers (who may be employed by non-profit or for-profit organizations) must apply to the RGE indicating the purpose and scope of a proposed research project.[161] Each application is reviewed by the RGE Review Committee, which consists of university faculty and RGE staff, as well as representatives from each of the suppliers of data to the UPDB (e.g., Utah Cancer Registry, Mormon church, Utah Department of Health, etc.).[162] The Review Committee reviews the application as a whole, giving particular attention to its data privacy and security plan.[163] In addition, any data contributor may "veto" the use of its data in any given project if they feel that the use is not appropriate.[164] Each user authorized to access UPDB data is required to sign a confidentiality agreement to protect individual-level data.[165]

157. Utah Exec. Order (Jul. 14, 1982).

158. Utah Exec. Order (Feb. 20, 1986).

159. *See supra* note 163-164 and accompanying text; *see also* Smith et al., *supra* note 147, at 12.

160. *See* Smith et al., *supra* note 147, at 9; *Utah Resource for Genetic & Epidemiologic Research (RGE)-Policies and Procedures,* U. UTAH, https://rge.utah.edu/policy_updb.php, (last visited Jan. 2, 2019) [hereinafter *RGE Policies*].

161. RGE Policies, *supra* note 160, Guidelines for Use of RGE-Held Data, Sec. I.

162. RGE Policies, *supra* note 160, Organization and Operation of the Resource; Smith et al., *supra* note 147, at 9; *Utah Resource for Genetic & Epidemiological Research (RGE)-RGE Review Committee*, U. UTAH https://rge.utah.edu/review_committee.php (last visited Jan. 2, 2019).

163. RGE Policies, *supra* note 160.

164. Smith et al., *supra* note 147, at 9.

165. *Id.*

Penalties for non-compliance with required confidentiality and other usage restrictions are set forth in the RGE Policies as follows:

> The RGE Director, using discretionary authority, may immediately suspend an authorization based upon behavior contrary to the best interests of the RGE or the data. The suspension will be in effect pending an investigation by the RGE Review Committee. Violations of any RGE rules, especially regarding data confidentiality, will subject the individual to the appropriate disciplinary response including suspension of user privileges, notification of the Institutional Review Board and the Office of the Associate Vice President for Research Integrity and Compliance, and, as appropriate faculty discipline (see Code of Faculty Responsibility) and investigation of possible violation of state law (see Utah Code Section 26-25-5).[166]

Thus, ensuring compliance with data usage requirements is incumbent on the RGE, acting as an agent of the state government on behalf of individual data subjects. Data subjects have no direct entitlement to prevent usage of data pertaining to themselves or to seek damages for misuse of such data. Penalties for non-compliance consist primarily of state-imposed debarment from further usage of the resource ("suspension of user privileges"), as well as internal administrative disciplinary procedures (e.g., for University of Utah faculty members), and potential state prosecution.[167] We are unaware of any instance in which such penalties have been sought or imposed.

By most measures the UPDB has been a success. The quantity and types of data that it links have steadily increased over the years of its operation. More importantly, use of UPDB data has led to hundreds of peer reviewed scientific publications, indicating that the availability of this resource has helped to advance scientific understanding.[168] With the increasing linkage of stored biospecimens with existing UPDB genealogical and statistical data, it is hoped that this resource will continue to be a valuable resource for the research community.

B. Statistics Denmark (DST)

Statistics Denmark (DST), a division of the Danish Ministry for Economic and Interior Affairs, has been a central authority for national

166. RGE Policies, *supra* note 160, Guidelines for Use of RGE-Held Data. Under the referenced statutory section (Utah Code 26-25-5), "[a]ny use, release or publication, negligent or otherwise, contrary to the provisions of [Chapter 26-25] is a class B misdemeanor."

167. *Id.*

168. *See Utah Population Database – Publications*, UNIV. UTAH, https://healthcare.utah.edu/huntsmancancerinstitute/research/updb/public ations/2016.php (last visited Jan. 2, 2019); Cannon Albright, *supra* note 147, at 210-214.

Danish statistics for more than 150 years and still produces official statistics relating to the Danish population, economy, culture, and environment.[169] This data, which includes a range of vital statistics (birth, death, marriage, divorce, etc.), is presented in a searchable, aggregated form on the DST web site[170] and is compiled in various agency reports. It is made available to the public at no charge and may be used for any purpose, so long as the data source is properly acknowledged.[171]

All Danish citizens are assigned a unique ten-digit civil registration (CPR) number.[172] The CPR number itself is associated with demographic information,[173] and also facilitates the combination of this data with other governmental registries covering health, education, employment, and income information on an individual level. Further, health data from both public and private encounters are routinely transferred to national registries using an individual's CPR number.[174] DST offers remote access to de-identified individual level data through CPR[175] for researchers at institutions authorized by DST.[176] Under Danish law, consent must in general be obtained for health-related research projects.[177] Research based solely on registry records, however, does not require individual consent and researchers can thus conduct purely registry-based research projects on the Danish population using the CPR number without the consent of the participant.[178]

169. STATISTICS DENMARK, https://www.dst.dk/en (last visited Mar. 8, 2019).

170. For example, users may compile data graphs and tables correlating annual data for variables such as age, fertility rate, cause of death, marital status, household income and immigration status. *See, e.g., Population and Elections*, STATISTICS DEN., https://www.dst.dk/en/Statistik/emner/befolkning-og-valg (last visited Jan. 17, 2018).

171. *General Terms—Open Data and Copyright*, STATISTICS DENMARK, https://www.dst.dk/en/OmDS/omweb (last visited Jan. 17, 2019).

172. Carsten Bøcker Pedersen, *The Danish Civil Registration System*, 39 SCANDINAVIAN J. PUB. HEALTH 22, 22-23 (2011).

173. *Id.*

174. *Id.*

175. Under the Danish Act on Processing of Personal Data, Act No. 429 of May 31, 2000, research results based on personal data may only be made available on an anonymized basis. Mette Hartlev, *Genomic Databases and Biobanks in Denmark*, 43 J.L. MED. & ETHICS 743, 749-751 (2015).

176. Lau Caspar Thygesen et al., *Introduction to Danish (Nationwide) Registers on Health and Social Issues: Structure, Access, Legislation, and Archiving*, 39 SCANDINAVIAN J. PUB. HEALTH 12, 14 (2011); *Data for Research*, STATISTICS DEN., https://www.dst.dk/en/TilSalg/Forskningsservice (last visited Jan. 17, 2019).

177. *See* Hartlev, *supra* note 175, at 745.

178. Folketinget. Bekendtgørelse af lov om videnskabsetisk behandling af sundhedsvidenskabelige forskningsprojekter. [The Danish Parliament:

In order to access and use individual level data from DST, researchers must sign a written researcher agreement that contains a number of conditions and restrictions on data use.[179] For example, researchers must agree to download only aggregated results (data, tables, figures) from DST's servers, and not to download individual-level data ("micro data") pertaining to individuals, households, families, or business entities, even if this data is accessible on the server.[180] DST offers as a rule of thumb that data transferred to a researcher's computer "should be aggregated to a level which can be used directly in a publication."[181]

DST also lays out a detailed set of penalties for violation of these policies. Thus, if DST observes that individual-level data have been transferred to a researcher's computer, it will immediately block all access to DST data by the researcher and its institution.[182] The researcher and its institution are then required to delete all files containing the improperly downloaded data, and the institution must prepare both an explanation of the violation and a remedial plan to avoid such violations in the future.[183] While DST is evaluating the matter, access to all DST data is closed to both the researcher and the institution.[184] If such violations recur, DST may limit or close access to the researcher and the institution for a longer period based on the severity of the violation and the number of prior incidents.[185] *Figure 1* below illustrates the hierarchy of severity and recurrence-based penalties for such data violations.

Ministerial Order on Scientific Treatment of Health Scientific Research Projects]. (Denmark 2017 [hereinafter Danish Ministerial Order]. *See also* Hartlev, *supra* note 175, at 746. It is the authors' understanding, based on Nordfalk's communications with DST, that the enactment of the GDPR will not require significant changes to DST's data access and usage policies. However, DST plans to implement a number of ministerial changes as a result of the GDPR. For example, DST's standard data usage agreement will no longer require that researchers report on their research to the Danish Data Protection Agency, as researchers will be directly responsible for their use and handling of data.

179. GUIDELINES FOR TRANSFERRING AGGREGATED RESULTS FROM STATISTICS DENMARK'S RESEARCH SERVICES, STATISTICS DEN. (2015) [hereinafter DST Guidelines].

180. *Id.*

181. *Id.*

182. *Id.* at 5.

183. *Id.*

184. *Id.* at 5-6.

185. *Id.* at 6-7.

Figure 1
Statistics Denmark Advisory Summary of Sanctions in Cases of a breach of the data confidentiality rules or data security[186]

	Sanctions against the institution			**Sanctions against the researcher**	
Transfer of data at the level of individuals	**1st time for the institution**	**2nd time for the institution**	**Repeated times for the institution**	**1st time**	**Several times**
Technical mistake which was not done deliberately	Quarantine of 1 month for the institution (may be considered a mitigating circumstance, if the mistake is reported by the authorized institution)	Quarantine of 2 months for the institution	Quarantine of 3 months for the institution	Quarantine of 1 month from all research projects (may be considered a mitigating circumstance, if the mistake is reported by the authorized institution)	Quarantine of 3 months from all research projects
Deliberate action – wanted to look at data (error detection)	Quarantine of 2 months for the institution	Quarantine of 3 months for the institution	Quarantine of 3 months for the institution	Quarantine of 2 months from all research projects	Permanent Exclusion
Deliberate attempts at identifying data	Quarantine of 3 months for the institution	Quarantine of 3 months for the institution	Permanent exclusion	Permanent exclusion	Cannot occur
Password or access passed on by the authorized person	**1st time for the institution**	**2nd time for the institution**	**Repeated times for the institution**	**1st time**	**Several times**
Carelessness	Quarantine of 1 month for the institution	Quarantine of 2 months for the institution	Quarantine of 3 months for the institution	Quarantine of 1 month from all research projects	Quarantine of 3 months from all research projects
Deliberately	Quarantine of 3 months for the institution	Quarantine of 3 months for the institution	Permanent exclusion	Quarantine of 3 months from all research projects	Permanent exclusion

As summarized in *Figure 1*, for an inadvertent mistake that has only occurred once, the researcher and institution may be barred from access to DST data for one month, while a deliberate attempt to derive personal identities from DST data will result in the permanent exclusion of the researcher. If the violation occurs three times within the same institution, the institution is barred from using all DST data.[187]

186. *Id.* at 7.

187. *Id.* at 7.

The framework that DST has implemented to deal with the use of its data relies on regulatory rules. While individual data subjects have no property-like entitlement to control the use of data once it has entered the DST database or to exclude researchers from using that data, DST itself imposes meaningful penalties on researchers and institutions that violate the cardinal rule of data access: no downloading of individual-level data. These penalties escalate based on the severity of the violation and the degree of recurrence.

The penalties that DST imposes are of the remediation and debarment varieties. Monetary penalties are not a part of the DST framework at this time. DST's remediation remedy requires the deletion of individual-level data that was improperly downloaded to a researcher's computer. This remedy is reasonable and appropriate given the outright prohibition on downloading this data. Moreover, this remedy should have little effect on legitimate use of the data, either by the affected institution or by others, as no bar is imposed on the continuing use of properly downloaded aggregate data. Thus, unlike a property rule system in which aggrieved data subjects could potentially disrupt compliant research use of data pertaining to themselves, the liability rule imposed by DST is narrowly focused on the offending data and parties.

Likewise, the debarment remedies available to DST are calculated to penalize, first, the noncompliant researcher and, in more serious or recurring cases, its institution. The escalating nature of these penalties is fitting as it assigns differing time periods for debarment based on severity and recidivism. Even "permanent" debarment for an individual or an institution, while harsher than most U.S. governmental debarment penalties, can be seen as justified given the high premium placed by DST on the privacy interests of its data subjects.

C. Lessons Learned from UPDB and DST

Both UPDB and DST make large quantities of individual health data available to researchers without obtaining specific consent from individual data subjects. Instead, the public custodians of the data assume the responsibility for ensuring that data users observe rules and restrictions regarding access to and use of the data. UPDB and DST have been able to proceed in this manner because they are maintained by governmental agencies operating, to differing degrees, outside of the general regulatory scheme for human subjects research. UPDB, as an arm of the Utah State Government that does not receive U.S. federal funding, does not operate under the strictures of the Common Rule, and DST operates under Danish national legislation that does not require consent for register-based research.[188]

However, as governmental agencies, UPDB and DST are themselves invested with a public interest role and can, as such, be

188. Danish Ministerial Order, *supra* note 178.

relied upon to safeguard the privacy and other interests of individuals whose data they maintain and make available. As a result, the need to obtain *ex ante* consent from every data subject is avoided with concomitant efficiency gains and cost savings. In turn, monitoring and enforcement are required, but this burden has been assumed by the state rather than individual data subjects.[189]

Another important feature of both of these frameworks is that private remedies, such as those asserted in *Beleno* and *Havasupai*, are excluded. As noted above, Utah law expressly shields those who provide "condition and treatment" data to researchers from civil liability, instead limiting remedies for data misuse to those specified under the RCE statute.[190] In Denmark (and under the GDPR) private remedies are also unavailable.[191] Thus, in both of these regimes, the extreme remedies sought in cases such as *Beleno* (destruction of 5.3 million infant blood spots) and *Havasupai* ($50 million in damages) are not available. *Table 4* below summarizes the remedy types authorized under the UPDB and DST frameworks:

Table 4
Remedies Authorized by UPDB and DST

Type of Remedy	UPDB	DST
Compensatory damages	No	No
Fines and penalties	No	No[192]
Remediation	Yes	Yes
Debarment	Yes	Yes
Institutional Sanction	Yes	No
Criminal Sanction	Yes	No

As noted above, the data access and usage frameworks established by the UPDB and DST are regulatory, rather than property or liability rules. Individual data subjects have no right to pre-approve uses of their validly-collected data, nor do they have a remedy in the event of unauthorized access or usage. Rather, the government, acting in the public interest, fulfills both of these roles: it determines, using a defined administrative process, who may access and use data, and on what terms they may do so. It also enforces compliance with its data access

189. *Cf.* Contreras, *Biomedical Data, supra* note 117, at 36-38 (discussing role of state in enforcing rules relating to public data access).

190. *See supra* note 150 and accompanying text.

191. *See* GDPR, *supra* note 29, at Article 83.

192. Significant fines may be imposed under the GDPR. *See* GDPR *supra* note 29.

and usage rules and levies penalties for non-compliance. These penalties, when warranted, may be harsh (e.g., permanent debarment of an institution from data access in the case of DST), but in all cases they are directed solely against the offending individuals and institutions, not more broadly against innocent researchers who have obtained and used the relevant data in accordance with applicable rules. As such, the likelihood that large-scale socially valuable research will be disrupted by the assertion of individual rights in data is substantially reduced.

This is not to say, of course, that establishing regulatory and liability rule regimes for the governance of data-based research will be easy or cost-free. Fashioning such a framework requires careful attention to potential threats to personal privacy that may arise from contemplated research, as well as prioritization of violations and formulation of remedies. In the U.S., general liability rules already exist to prohibit abuses of genetic data by employers and insurers under GINA, to protect patients from unauthorized use of data by physicians, and to redress injuries caused by violation of privacy laws.[193] Data custodians such as UPDB have additional protections for the data that they make available, including strict requirements regarding data confidentiality. DST imposes serious penalties for downloading individual-level data from its servers. Data custodians in other jurisdictions may establish different priorities and penalties.[194] Yet the diversity that may emerge across systems should not be viewed negatively. Differences in policy design indicate a system that is working to tailor requirements to the needs of its stakeholders. It is the "one size fits all" property rule framework that creates results that are often inappropriate and mismatched to the needs of individual systems.

Once a framework for data access and usage is in place, monitoring of compliance and enforcement against violators is required.[195] Though default allocation rules would typically place this monitoring and compliance burden on individual data subjects, in the UPDB and DST cases the state has shifted these burdens to a public authority.[196] This allocation is likely efficient, as individual data subjects are in a comparatively weak position to detect noncompliance with data access

193. *See* Contreras, *Genetic Property, supra* note 15, at 41-43 (discussing liability rules).

194. *See, e.g.,* David Cyranoski, *China Cracks Down on Genetics Breaches*, 563 NATURE 301, 301 (2018) (describing Chinese Ministry of Science enforcement actions against institutions violating genetic data sharing rules).

195. For a more detailed discussion of monitoring and enforcement costs in the context of genetic data regulation, see Contreras, *Genetic Property, supra* note, 15, at 48-51.

196. Hartlev, *supra* note 175, at 747; UTAH CODE ANN. § 26-3-10 (LexisNexis 2017).

and usage rules [197] This shift also satisfies general notions of fairness and equity as the government is charged with safeguarding individual interests and privacy.[198] Of course, allocating these burdens to the data custodian (whether a state agency, a university or other research institution) increases the cost borne by these institutions. But, if the advancement of biomedical research is a priority for the state, then it is not unreasonable to expect the state to allocate sufficient resources to cover these monitoring and enforcement costs.[199]

IV. Conclusions

The recent trend toward the propertization of human genetic and other health data under U.S. law poses significant challenges to large-scale biomedical research and public health. Property rule systems can result in sizable up-front costs in the *ex ante* acquisition of informed consent from individual data subjects, as well as the ongoing risk that data subjects will retract consent or object to unanticipated data uses, thus compromising existing data resources and analyses.

We argue that liability rule and regulatory frameworks, in which data-based research is permitted but researchers are subject to penalties for impermissible data access or usage, can offer robust protection of individual data privacy and security while better promoting the integrity of the research enterprise and reducing inefficiencies associated with the acquisition of consent from large numbers of data subjects. We propose that research using individual health data should be subject to a regulatory regime, enforceable by government/public repositories, while at the same time permitting limited private enforcement actions to address particularized individual injury. Thus, though the physical collection of human tissue would continue to be subject to existing rules regarding informed consent, *ex ante* consent would *not* be required for the use of information derived from physical samples. Rather, rules regarding proper research use of health information would be put in place, and violations of those rules could be dealt with on an *ex post* basis, both through regulatory penalties and private actions.

197. It is not always the case that individual data subjects will remain unaware of alleged rule violations, as the private actions brought in the *Beleno* and *Havasupai* cases demonstrate. Beleno v. Lakey, 306 F.Supp.3d 930, 936-7 (2009); Havasupai Tribe v. Ariz. Bd. of Regents, 204 P.3d 1063, 1066 (Ariz. Ct. App. 2008).

198. Thus, while shifting the monitoring and enforcement burden to a private firm might not seem equitable, even if it were efficient, shifting the burden from individuals to a public authority that acts on behalf of its citizens, does not raise the same equity issues.

199. For examples of state-led initiatives in making biomedical data broadly available and the multifaceted role of the state in such initiatives, see Contreras, *supra* note 116, at 39.

Our recommendations are supported by two cases studies: the Utah Population Database and Statistics Denmark, both of which provide examples of successful health data repositories that are governed by regulatory systems. While both of these examples are drawn from governmental data resources, the approach that they exemplify, and their limitations on private causes of action, can be extended to academic and other research environments. We thus recommend that such regulatory models be considered more broadly for the governance of research using human health data.